25th Anniversary

IUG2017

NATIONAL HARBOR | MARYLAND

25TH ANNUAL INNOVATIVE USERS GROUP CONFERENCE

APRIL 2-5, 2017

Protecting Patrons' Privacy

Phil Shirley
Cuyahoga Falls Library

Preface

Library Freedom Project

- libraryfreedomproject.org
- @libraryfreedom

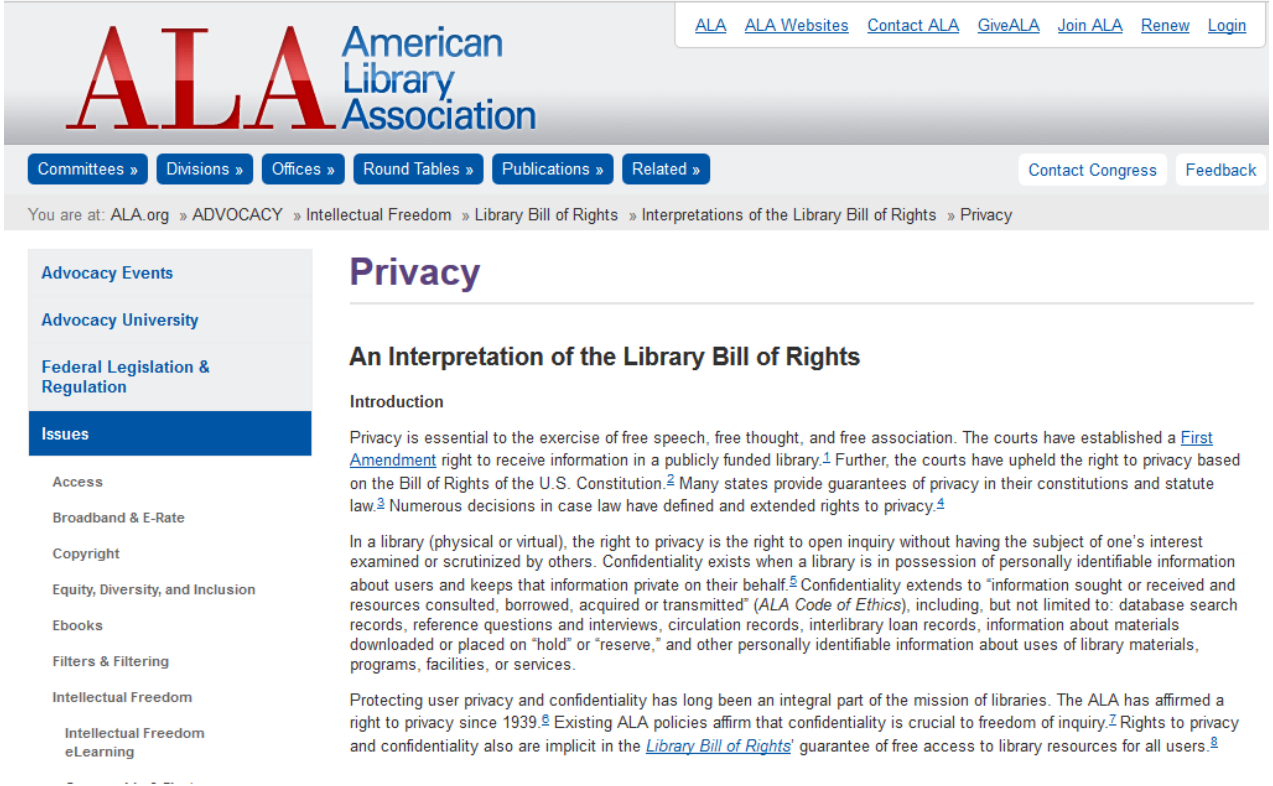
ACLU

AMERICAN CIVIL LIBERTIES UNION

EFF

ELECTRONIC FRONTIER FOUNDATION

Tor



ALA American Library Association

[ALA](#) [ALA Websites](#) [Contact ALA](#) [GiveALA](#) [Join ALA](#) [Renew](#) [Login](#)

Committees » Divisions » Offices » Round Tables » Publications » Related » Contact Congress Feedback

You are at: ALA.org » ADVOCACY » Intellectual Freedom » Library Bill of Rights » Interpretations of the Library Bill of Rights » Privacy

- Advocacy Events
- Advocacy University
- Federal Legislation & Regulation
- Issues
  - Access
  - Broadband & E-Rate
  - Copyright
  - Equity, Diversity, and Inclusion
  - Ebooks
  - Filters & Filtering
  - Intellectual Freedom
    - Intellectual Freedom eLearning

Privacy

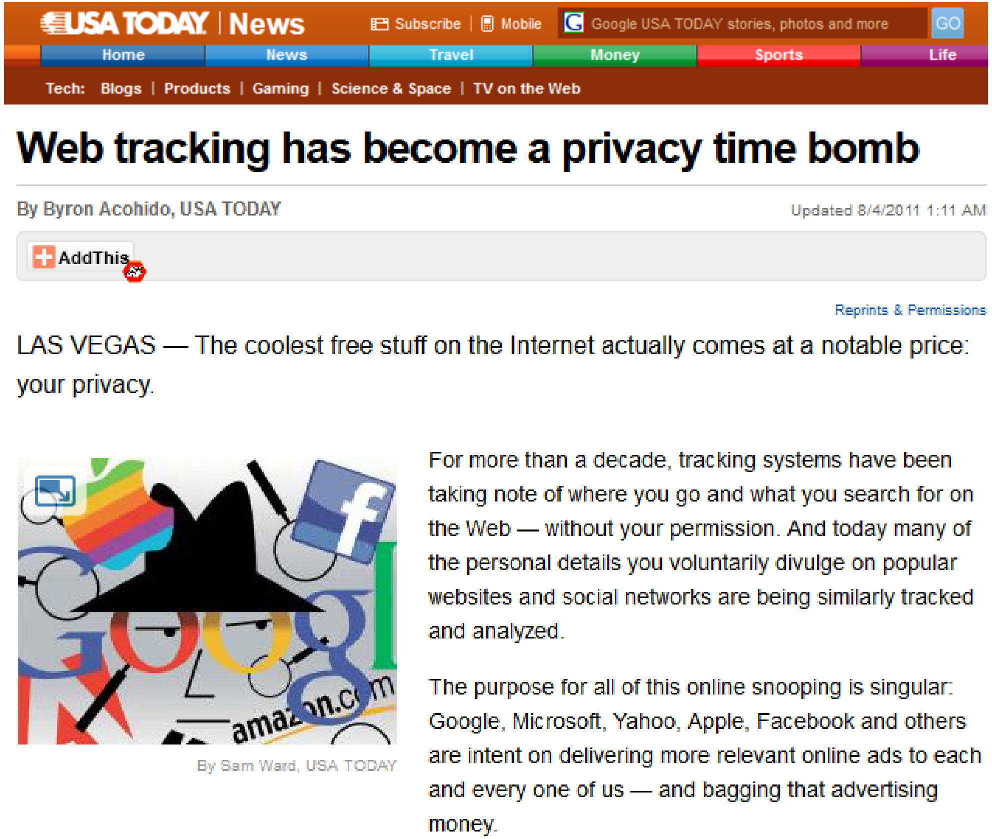
An Interpretation of the Library Bill of Rights

Introduction

Privacy is essential to the exercise of free speech, free thought, and free association. The courts have established a First Amendment right to receive information in a publicly funded library.[1] Further, the courts have upheld the right to privacy based on the Bill of Rights of the U.S. Constitution.[2] Many states provide guarantees of privacy in their constitutions and statute law.[3] Numerous decisions in case law have defined and extended rights to privacy.[4]

In a library (physical or virtual), the right to privacy is the right to open inquiry without having the subject of one's interest examined or scrutinized by others. Confidentiality exists when a library is in possession of personally identifiable information about users and keeps that information private on their behalf.[5] Confidentiality extends to "information sought or received and resources consulted, borrowed, acquired or transmitted" (*ALA Code of Ethics*), including, but not limited to: database search records, reference questions and interviews, circulation records, interlibrary loan records, information about materials downloaded or placed on "hold" or "reserve," and other personally identifiable information about uses of library materials, programs, facilities, or services.

Protecting user privacy and confidentiality has long been an integral part of the mission of libraries. The ALA has affirmed a right to privacy since 1939.[6] Existing ALA policies affirm that confidentiality is crucial to freedom of inquiry.[7] Rights to privacy and confidentiality also are implicit in the *Library Bill of Rights*' guarantee of free access to library resources for all users.[8]



USA TODAY | News
Subscribe | Mobile
Google USA TODAY stories, photos and more
GO
Home
News
Travel
Money
Sports
Life
Tech: Blogs | Products | Gaming | Science & Space | TV on the Web

Web tracking has become a privacy time bomb

By Byron Acohido, USA TODAY

Updated 8/4/2011 1:11 AM

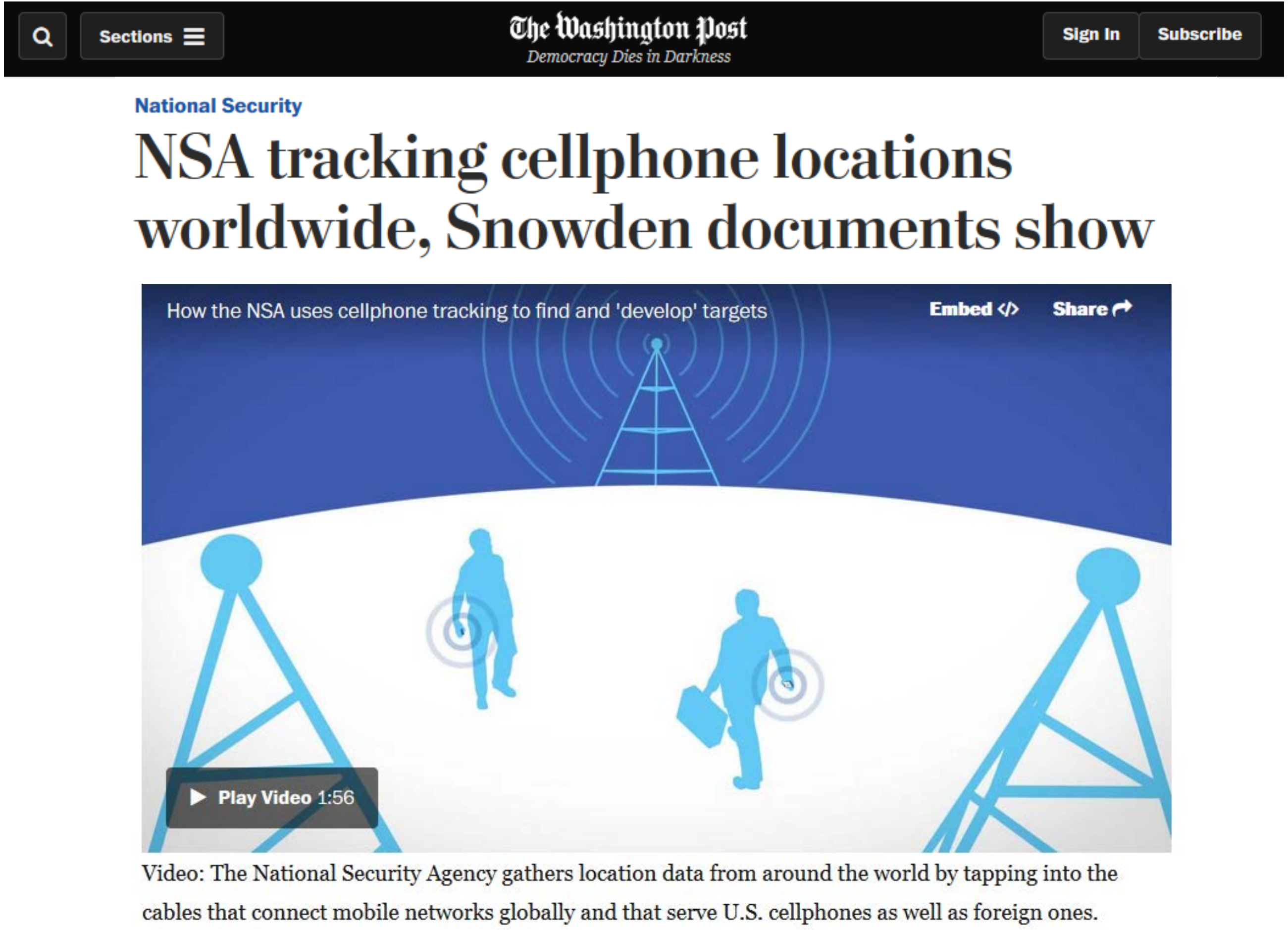
AddThis
Reprints & Permissions

LAS VEGAS — The coolest free stuff on the Internet actually comes at a notable price: your privacy.

By Sam Ward, USA TODAY

For more than a decade, tracking systems have been taking note of where you go and what you search for on the Web — without your permission. And today many of the personal details you voluntarily divulge on popular websites and social networks are being similarly tracked and analyzed.

The purpose for all of this online snooping is singular: Google, Microsoft, Yahoo, Apple, Facebook and others are intent on delivering more relevant online ads to each and every one of us — and bagging that advertising money.

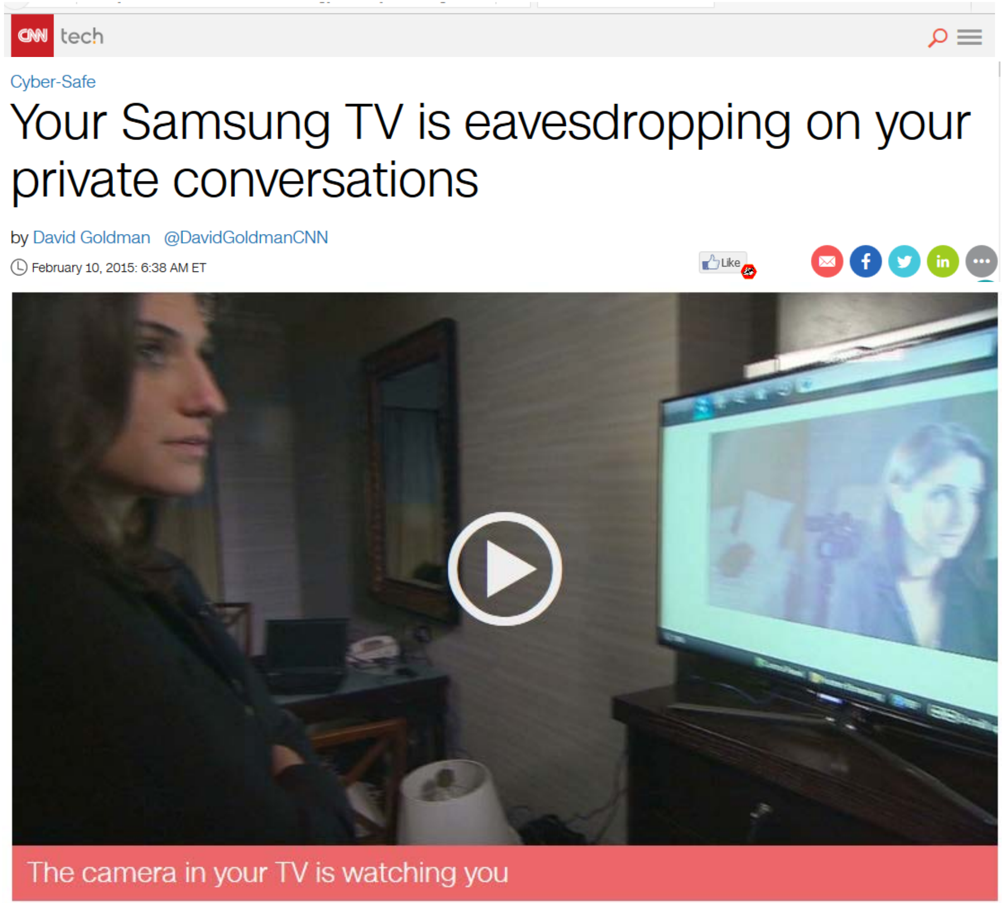

Sections
Sign In
Subscribe
How the NSA uses cellphone tracking to find and 'develop' targets
Embed
Share
Play Video 1:56

The Washington Post
Democracy Dies in Darkness

National Security

NSA tracking cellphone locations worldwide, Snowden documents show

Video: The National Security Agency gathers location data from around the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones.



CNN tech

Cyber-Safe

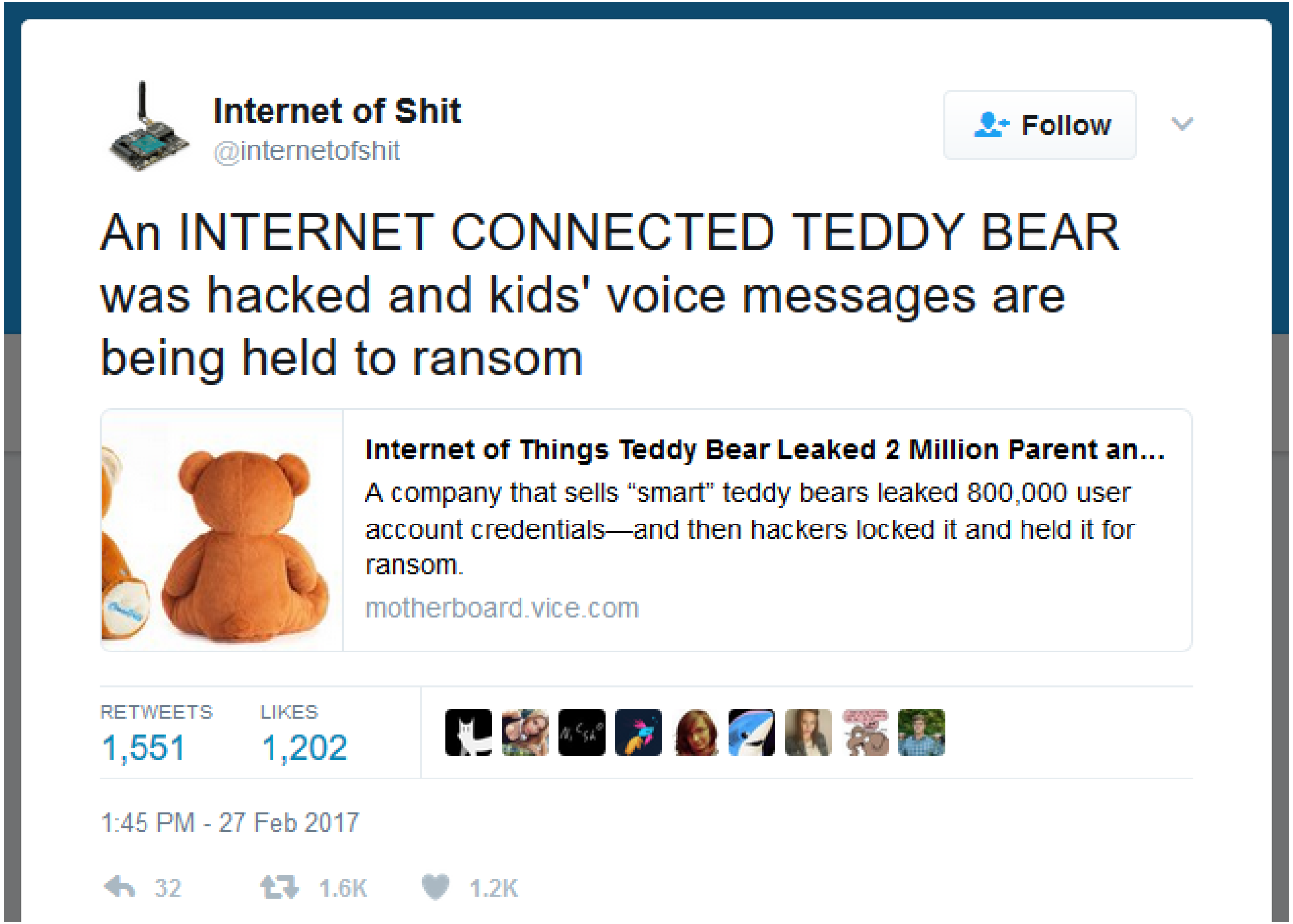
Your Samsung TV is eavesdropping on your private conversations

by David Goldman @DavidGoldmanCNN

February 10, 2015: 6:38 AM ET

Like

The camera in your TV is watching you



Internet of Shit
@internetofshit

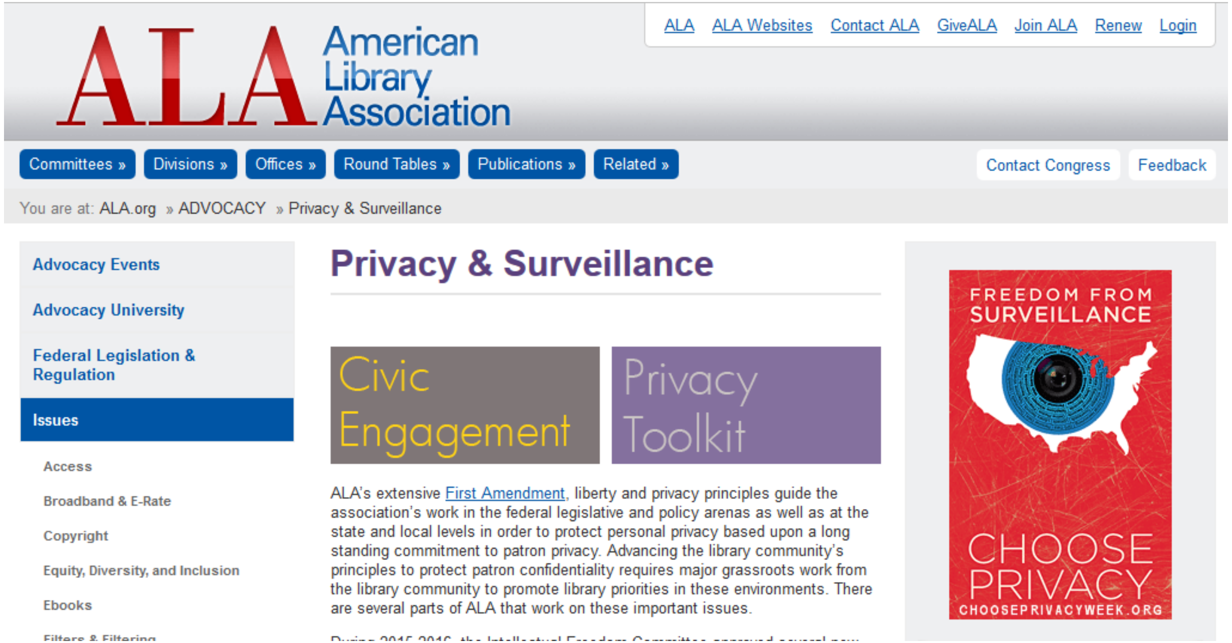
An INTERNET CONNECTED TEDDY BEAR was hacked and kids' voice messages are being held to ransom

Internet of Things Teddy Bear Leaked 2 Million Parent an...
A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.
motherboard.vice.com

RETWEETS	LIKES
1,551	1,202

1:45 PM - 27 Feb 2017

ala.org/advocacy/privacyconfidentiality



ALA American Library Association

ALA | ALA Websites | Contact ALA | GiveALA | Join ALA | Renew | Login

Committees » | Divisions » | Offices » | Round Tables » | Publications » | Related » | Contact Congress | Feedback

You are at: ALA.org » ADVOCACY » Privacy & Surveillance

- Advocacy Events
- Advocacy University
- Federal Legislation & Regulation
- Issues
  - Access
  - Broadband & E-Rate
  - Copyright
  - Equity, Diversity, and Inclusion
  - Ebooks
  - Filters & Filtering

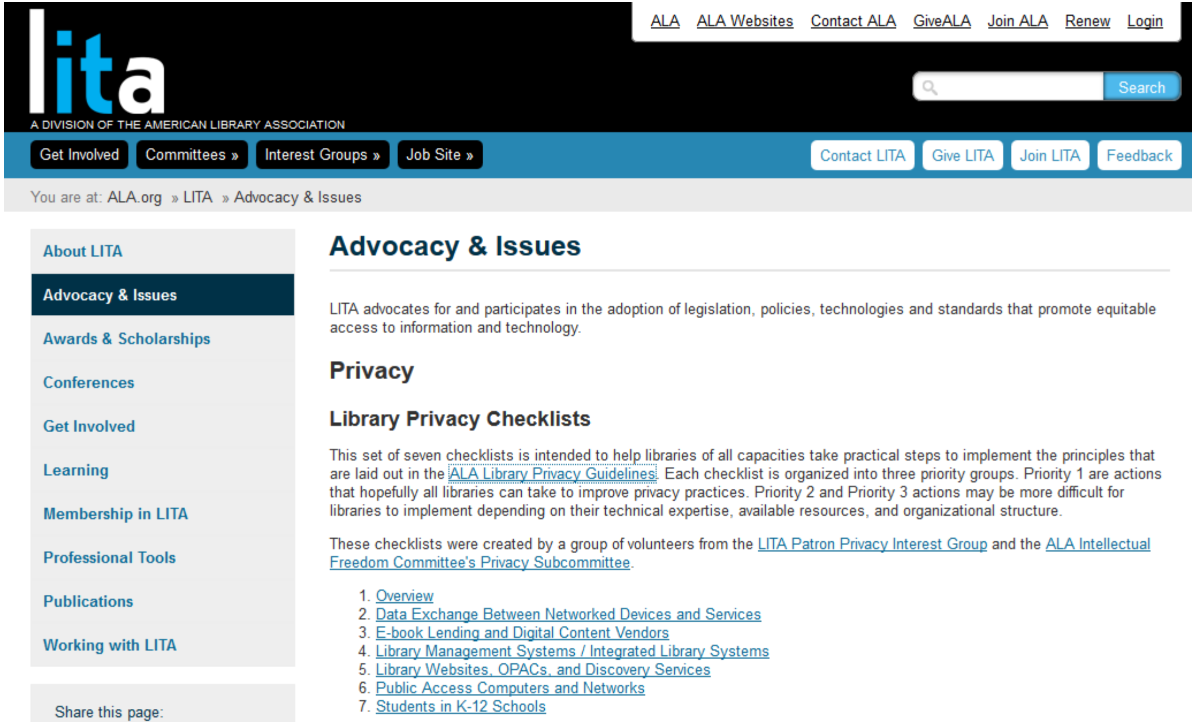
Privacy & Surveillance

Civic Engagement | Privacy Toolkit

ALA's extensive First Amendment, liberty and privacy principles guide the association's work in the federal legislative and policy arenas as well as at the state and local levels in order to protect personal privacy based upon a long standing commitment to patron privacy. Advancing the library community's principles to protect patron confidentiality requires major grassroots work from the library community to promote library priorities in these environments. There are several parts of ALA that work on these important issues.

During 2015-2016, the Intellectual Freedom Committee approved several new

ala.org/lita/advocacy



Advocacy & Issues

LITA advocates for and participates in the adoption of legislation, policies, technologies and standards that promote equitable access to information and technology.

Privacy

Library Privacy Checklists

This set of seven checklists is intended to help libraries of all capacities take practical steps to implement the principles that are laid out in the ALA Library Privacy Guidelines. Each checklist is organized into three priority groups. Priority 1 are actions that hopefully all libraries can take to improve privacy practices. Priority 2 and Priority 3 actions may be more difficult for libraries to implement depending on their technical expertise, available resources, and organizational structure.

These checklists were created by a group of volunteers from the LITA Patron Privacy Interest Group and the ALA Intellectual Freedom Committee's Privacy Subcommittee.

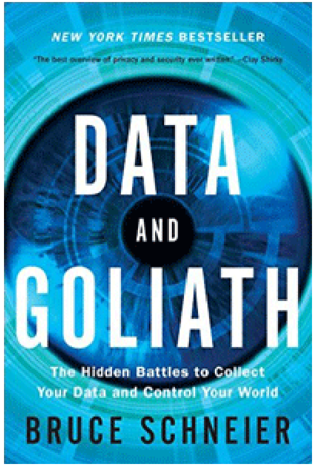
1. Overview
2. Data Exchange Between Networked Devices and Services
3. E-book Lending and Digital Content Vendors
4. Library Management Systems / Integrated Library Systems
5. Library Websites, OPACs, and Discovery Services
6. Public Access Computers and Networks
7. Students in K-12 Schools

Overview

- Does privacy matter?
- Classes: Protecting Yourself Online
- Our Systems
- Third Parties

Bruce Schneier

- Internationally renowned security technologist
- *Data and Goliath* (and many others)
- schneier.com
- @schneierblog


NEW YORK TIMES BESTSELLER
"The best overview of privacy and security ever written." —Clay Shirky
DATA
AND
GOLIATH
The Hidden Battles to Collect Your Data and Control Your World
BRUCE SCHNEIER

What if Privacy is Compromised?

- Identity Theft
- Harassment by Government
- Unintended Consequences

Internet Risks

- Web tracking
- Free services sell your data.
- Oversharing
- Misunderstanding privacy settings
- Changes in privacy policies
- Security compromise

Classes for the Public

Public Classes

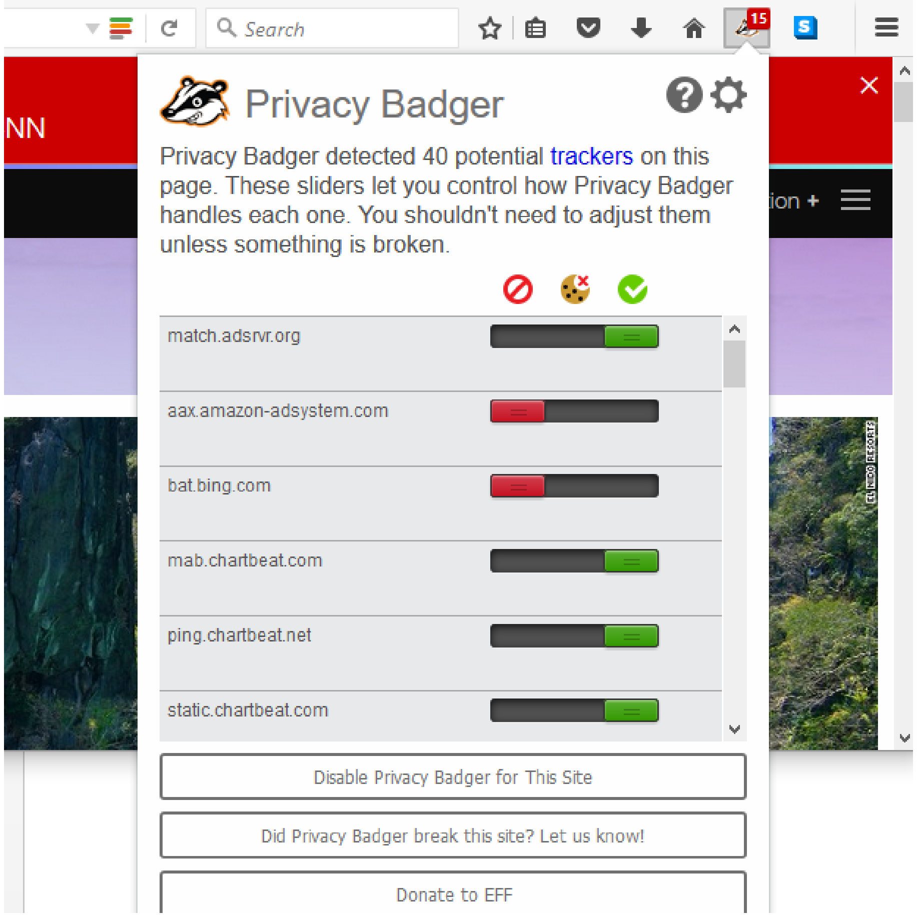
- Web safety 101
- More advanced topics
  - Choice of browser
  - Privacy Badger
  - TOS;DR
  - NoScript
  - HTTPS Everywhere
  - Tor Browser
  - Signal
  - VPNs
  - Password managers
  - Two-factor authentication
  - Private email providers
  - Private search engines
  - Lying

Choice of Browser

- Who do you trust?
- Security features of Chrome
  - Safe Browsing
  - Sandboxing
  - Auto updates

Privacy Badger

- Add-on for Firefox and Chrome
- From Electronic Frontier Foundation
- Blocks third-party trackers
- You can override it.



Search
15
NN
ion +
Disable Privacy Badger for This Site
Did Privacy Badger break this site? Let us know!
Donate to EFF

Privacy Badger

Privacy Badger detected 40 potential trackers on this page. These sliders let you control how Privacy Badger handles each one. You shouldn't need to adjust them unless something is broken.

	⊘	🍪	✓
match.adsrvr.org			●
aax.amazon-adsystem.com	●		
bat.bing.com	●		
mab.chartbeat.com			●
ping.chartbeat.net			●
static.chartbeat.com			●

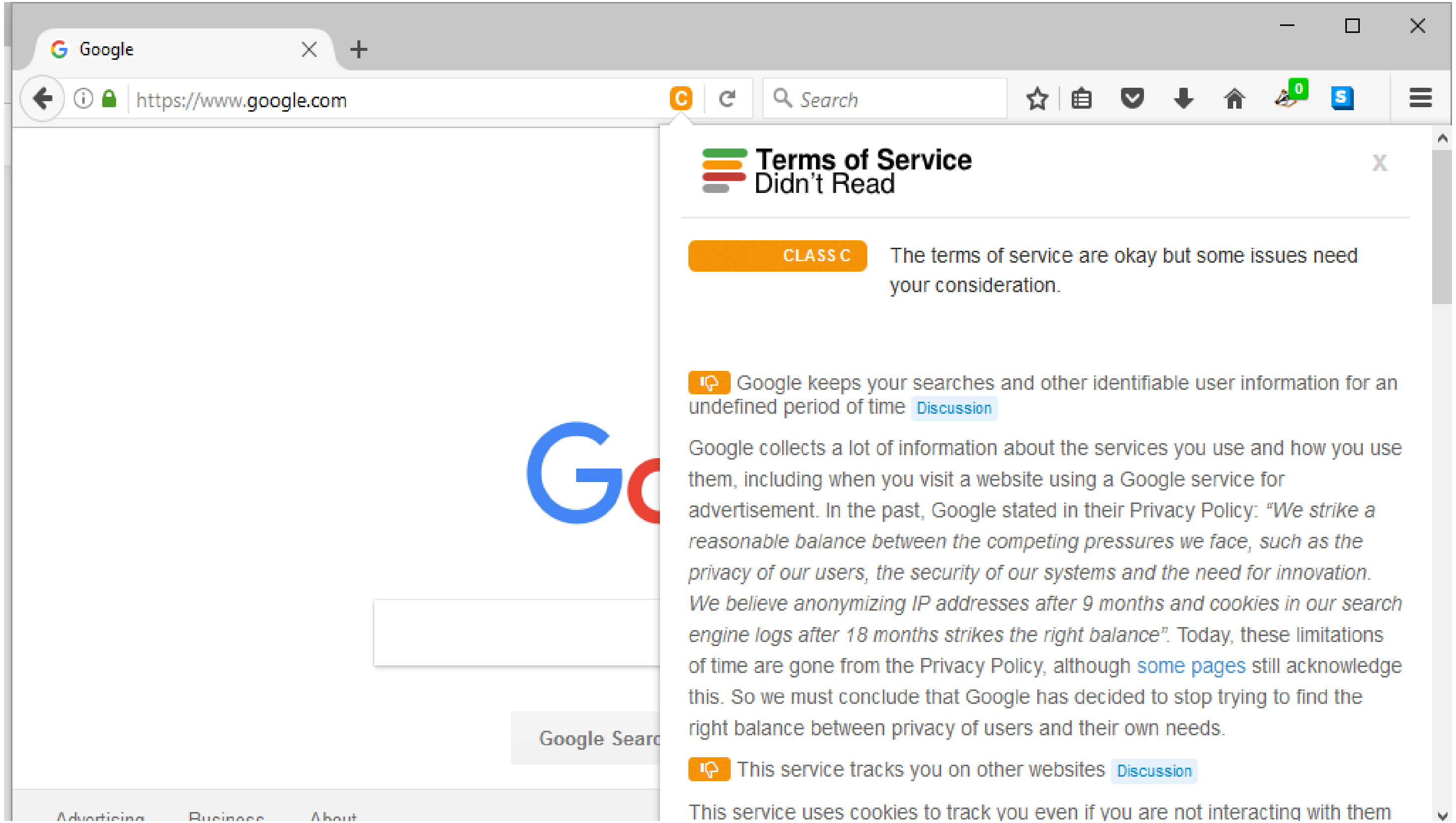
Terms of Service; Didn’t Read

- Add-on for Firefox, Chrome, Safari, and Opera
- Gives a summary and sometimes a class
- A play on “TL;DR”

Terms of Service; Didn’t Read

- Only some major web sites

https://tosdr.org/index.html#services



Terms of Service
Didn't Read

CLASS C The terms of service are okay but some issues need your consideration.

Google keeps your searches and other identifiable user information for an undefined period of time Discussion

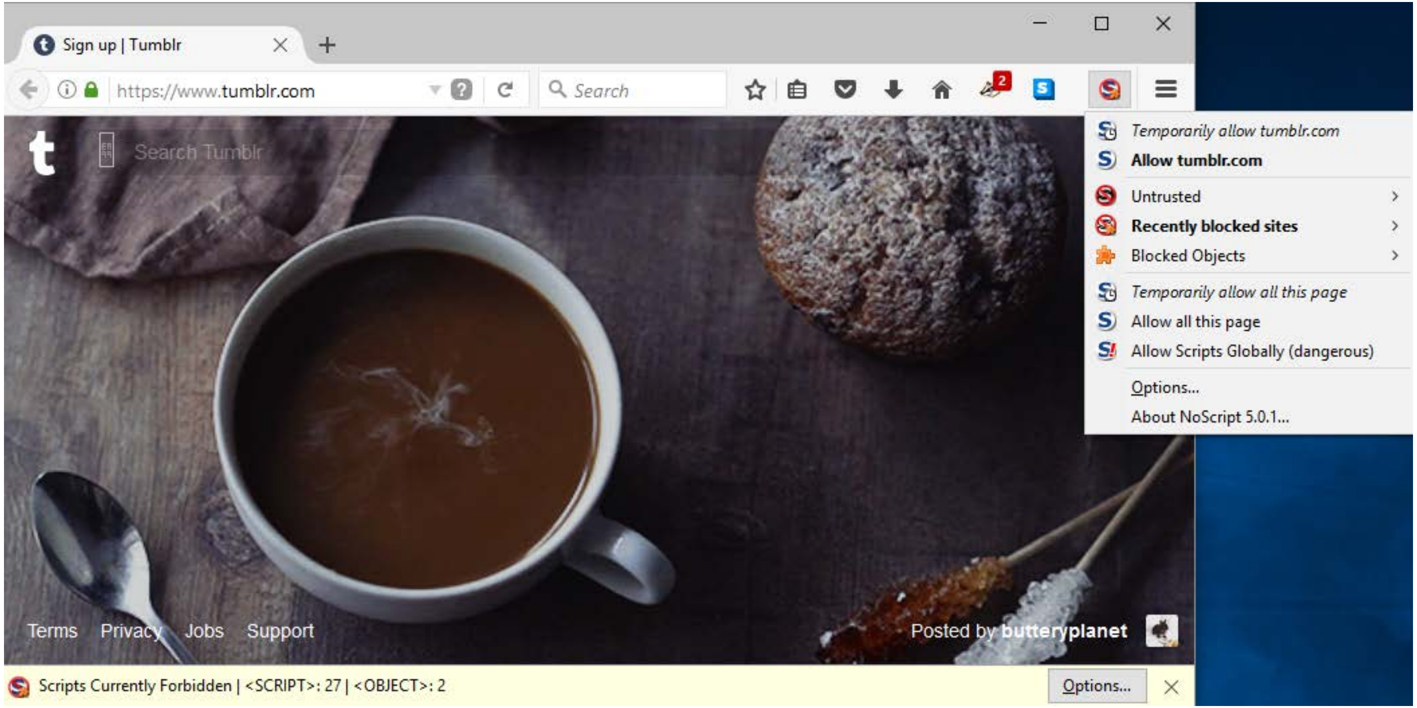
Google collects a lot of information about the services you use and how you use them, including when you visit a website using a Google service for advertisement. In the past, Google stated in their Privacy Policy: *"We strike a reasonable balance between the competing pressures we face, such as the privacy of our users, the security of our systems and the need for innovation. We believe anonymizing IP addresses after 9 months and cookies in our search engine logs after 18 months strikes the right balance"*. Today, these limitations of time are gone from the Privacy Policy, although some pages still acknowledge this. So we must conclude that Google has decided to stop trying to find the right balance between privacy of users and their own needs.

This service tracks you on other websites Discussion

This service uses cookies to track you even if you are not interacting with them

NoScript

- Add-on for Firefox
- Blocks Javascript, Java, Flash, etc.
- Default whitelist very short
- Whitelist or temporarily allow a site
- Provides other defenses



Scripts Currently Forbidden | <SCRIPT>: 27 | <OBJECT>: 2

HTTPS Everywhere

- Add-on for Firefox, Chrome, and Opera
- Takes you to secure version of site if there is one (for many sites)
- Free, open source
- Developed by EFF and Tor Project

HTTPS Ensures

- Confidentiality
- Authenticity
- Integrity

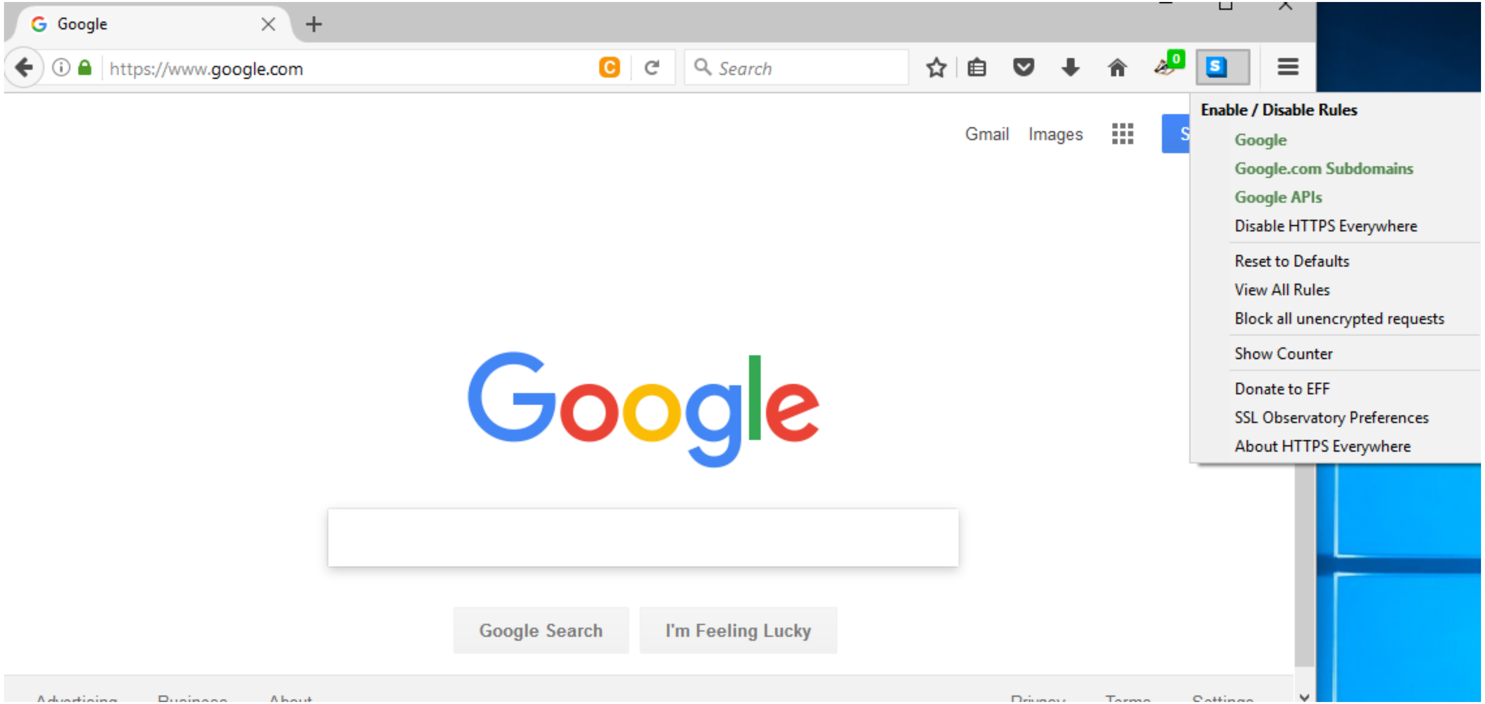
HTTPS Does not Protect

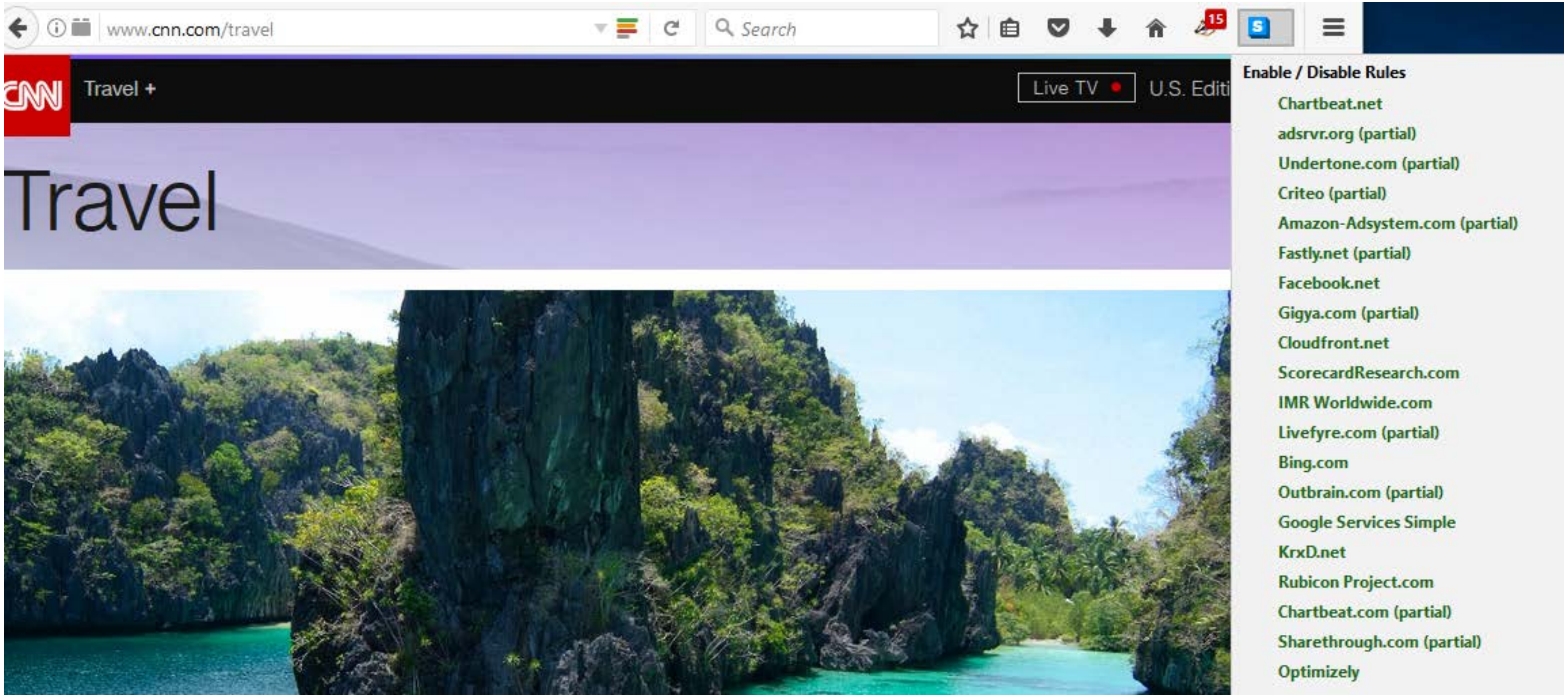
- DNS requests
- Domain names
- How long you’re on the site
- The relative size of user input

  – Per https://https.cio.gov/faq/

Not Just for Logging In

- Easier now
- Cheaper now (even free)
- Use it for everything
- EFF “What Every Librarian Needs to Know About HTTPS”


Google
https://www.google.com
Search
Gmail
Images
Google
Google Search
I'm Feeling Lucky
Enable / Disable Rules
Google
Google.com Subdomains
Google APIs
Disable HTTPS Everywhere
Reset to Defaults
View All Rules
Block all unencrypted requests
Show Counter
Donate to EFF
SSL Observatory Preferences
About HTTPS Everywhere


www.cnn.com/travel
Search
15
CNN
Travel +
Live TV
U.S. Editi
Travel
Enable / Disable Rules
Chartbeat.net
adsrvr.org (partial)
Undertone.com (partial)
Criteo (partial)
Amazon-Adsystem.com (partial)
Fastly.net (partial)
Facebook.net
Gigya.com (partial)
Cloudfront.net
ScorecardResearch.com
IMR Worldwide.com
Livefyre.com (partial)
Bing.com
Outbrain.com (partial)
Google Services Simple
KrxD.net
Rubicon Project.com
Chartbeat.com (partial)
Sharethrough.com (partial)
Optimizely

Tor Browser

- Web browser
- Routes traffic through Tor network
- Keeps secret what sites you visit
- Keeps sites from knowing your location
- Lets you access blocked sites

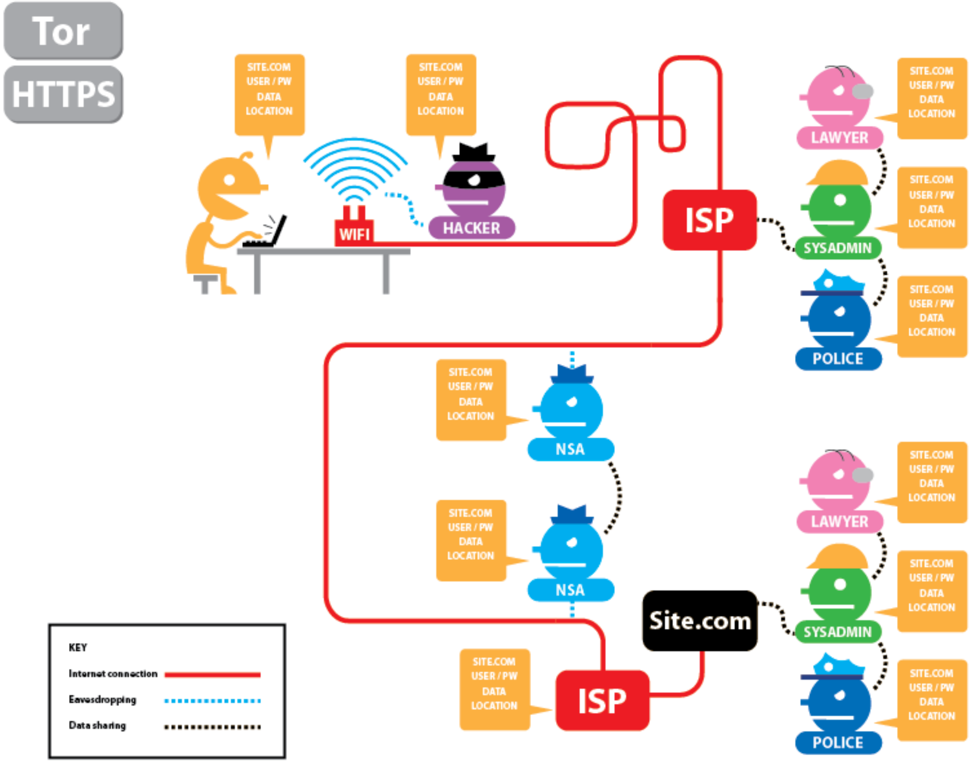
Tor Browser

- Based on same code as Firefox
- For Windows, Mac, Linux
- Portable (no need to install)
- Includes NoScript and HTTPS Everywhere

Tor Browser

- Slightly slower
- Be careful with banking or shopping sites

EFF Tor and HTTPS



https://www.eff.org/pages/tor-and-https

Encrypt Your Email

- Nope

Signal

- Android, iOS; Chrome app
- Encrypts calls and texts
- From Open Whisper Systems

Choosing a Email Provider

- Such as Riseup.net
- Encrypted end-to-end
- Doesn’t log your IP address
- Maybe two-factor authentication

Virtual Private Networks (VPNs)

- Shields your traffic from your ISP
- Good if you’re on a public wireless network

Password Managers

- Create super-secure passwords for you
- You supply one master password
- LastPass
- 1Password
- Start small

Two-Factor Authentication (2FA)

- Requires a password and something else
- Example: You get a text with a code to type in
- Many services support this

Choosing a Search Engine

- DuckDuckGo.com
- StartPage.com

False Information

- Give a fake date of birth?
- Usually breaks the terms of service

System Administration

The Essentials

- Principle of Least Privilege
- Keep OS, software, firmware up to date
- Password policies
- Server “hardening”
- Physical security
- Encrypt sensitive data

Library Policies

- LITA checklist 1
- Don’t collect more info than you need
- Don’t keep it longer than you need
- Sharing of information
- Requests from law enforcement

Setup of Public Computers

- Tor Browser
- Chrome and Firefox add-ons, disabled
    - Privacy Badger
    - HTTPS Everywhere
    - NoScript
- Desktop link to instructions & other privacy info

Setup of Public Computers

- Deep Freeze or similar
- Logs in Cassie or similar
- Privacy screens

Setup of Public Wifi

- Open vs. secure
- Isolation mode
- Logs

The Weakest Link: People

- Social engineering
- *How to Disappear* by Frank Ahearn

The ILS

Other Sessions

- Security and Compliance Primer for Innovative Libraries
- Maintaining Sierra Passwords and Privacy

Password Policies

- Require a new user to change password
- Maximum password age
- Complexity requirements
- Password history requirement
- Block after *x* unsuccessful attempts
- Can exempt certain users

User Permissions

- Apply the principle of least privilege

Limit Data Collected

- Consider adult or juvenile instead of birth date
- Is it necessary to collect a given piece of information?

Dangers of Having Data

- Data theft / hacking
- Government
- Accidents
- Staff

Limit Data Retention Period

- Specified in data retention policy
- Delete old patron records
- Delete long-billed items
- Delete ILL records

Circ Transaction File

- Details of checkouts, etc.
- In Sierra, access through SQL
- Defaults to two weeks
- Can be changed

WebPac and Encore

- Use HTTPS
- Require a PIN
- Allow patrons to change PIN
- Reading history

Notices

- Delete Teleforms history after gathering stats
- Don’t leave a detailed phone message
- Secure mailers

Email Notices

- “Email is a post card.”
- Not encrypted
- Includes home address?
- Includes title?
- CC feature

Other Things We Email

- Preferred Searched notifications (with titles)
- Other?

An Alternative to Email?

- Mobile app?
  - With notifications
  - With preferred search capability

Patron API (URL)

- Request a URL
  http://yourlibrary.org:4500/PATRONAPI/99999999999999/dump
  https://yourlibrary.org:54620/PATRONAPI/99999999999999/dump
- Get over three dozen fields, including
  - Name
  - Address
  - Phone number
  - Date of birth
  - PMESSAGE
  - Money Owed
  - Notes

Serucing Paton API

- Have Innovative remove some variable-length fields (maybe address, phone number, date of birth, notes)
- Use only HTTPS
  - Don’t give out the HTTP address
  - Use Limit Network Access and/or your firewall

Limit Network Access

- Patron API: HTPATAPI
- Patron API HTTPS: HTPATAPISSL
- “Local” address: First 3 octets the same (192.168.0._)
- Logs successes and failures

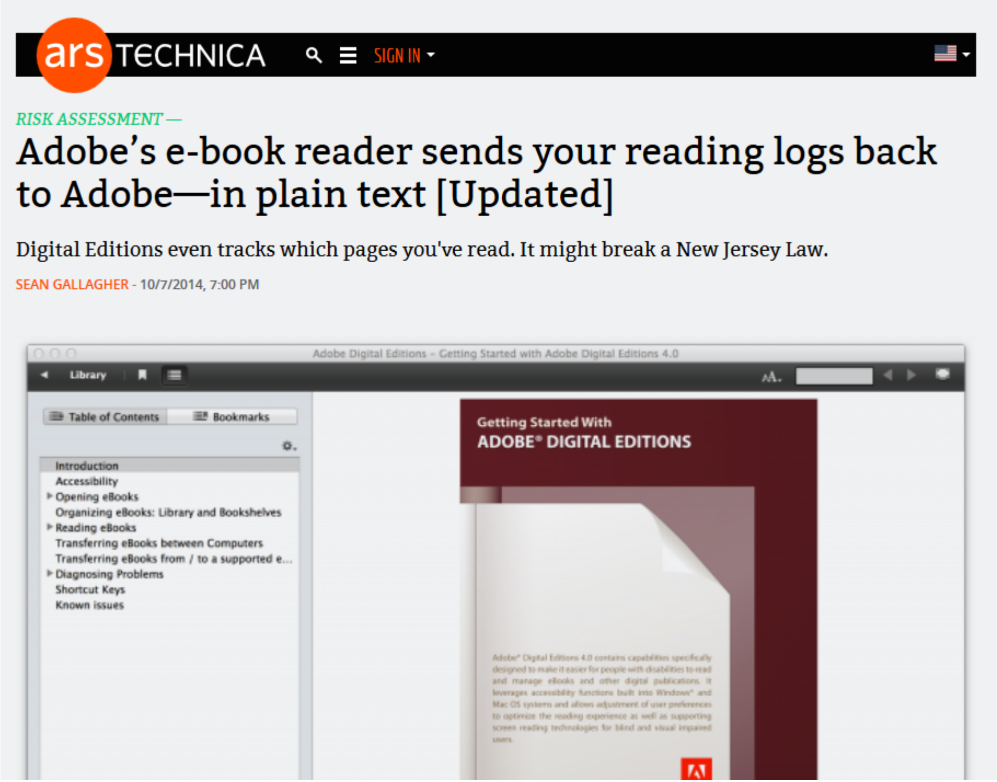
Firewall

- Don’t allow access to port 4500
- Restrict access to HTTPS port by IP address

Third Parties

Third Parties

- Library sends patron data to them
- Patrons give them their data
- Can track patrons’ searching and reading
- Can track patrons’ web use
- Can track patrons through app on phones or tablets


ars TECHNICA
SIGN IN
Adobe Digital Editions – Getting Started with Adobe Digital Editions 4.0
Library
Table of Contents
Bookmarks
Introduction
Accessibility
Opening eBooks
Organizing eBooks: Library and Bookshelves
Reading eBooks
Transferring eBooks between Computers
Transferring eBooks from / to a supported e...
Diagnosing Problems
Shortcut Keys
Known issues

RISK ASSESSMENT —

Adobe's e-book reader sends your reading logs back to Adobe—in plain text [Updated]

Digital Editions even tracks which pages you've read. It might break a New Jersey Law.

SEAN GALLAGHER - 10/7/2014, 7:00 PM

Getting Started With
ADOBE® DIGITAL EDITIONS

Adobe® Digital Editions 4.0 contains capabilities specifically designed to make it easier for people with disabilities to read and manage eBooks and other digital publications. It leverages accessibility functions built into Windows® and Mac OS systems and allows adjustment of user preferences to optimize the reading experience as well as supporting screen reading technologies for blind and visual impaired users.

https://arstechnica.com/security/2014/10/adobes-e-book-reader-sends-your-reading-logs-back-to-adobe-in-plain-text/

Library Checklist 3: Top Priorities

- Link to company’s privacy policy
- Try for opt-in collection of personal data
- Help patrons manage their privacy
- If data breach, notify patrons and help them mitigate damage

Library Checklist 3: 2nd Priorities

- Add privacy considerations to vendor selection criteria
- Think about privacy when reviewing agreements
  - Should comply with all laws
  - Library retains ownership of data
  - Patrons can access, correct, delete data about them

Library Checklist 3: 3rd Priorities

- Review agreements with current vendors
- Review vendors’ data governance plans
  - Patron consent
  - Data security
  - Encryption
  - Anonymization

Library Checklist 3: 3rd Priorities

- Review vendors' data governance plans
  - Retention
  - Dissemination / data sharing
  - Destruction
- Request regular privacy audits

Log In with Facebok

- What you’ve liked
- Birthday
- Hometown or current location
- Work history
- Friends list

https://developers.facebook.com/docs/facebook-login/overview/

Cloud Software and Patron Data

- G Suite (Gmail, Google Docs, etc.)
- Dropbox
- Anything else with patron data

Cloud Software and Patron Data

- Innovative Interfaced, Inc.
- ISO 27001 certified
- Information security standard
- For their hosted and cloud infrastructure

Other

Something Else You Could Do

- Provide Tor relay or exit nodes
  - Kilton Public Library (Lebanon, New Hampshire)
  - University of Western Ontario

Summary

Conclusion

Questions?

pshirley@fallslibrary.org